**AMENDMENTS TO THE CLAIMS:**

Without prejudice, this listing of the claims replaces all prior versions and listings of the claims in the present application:

**LISTING OF CLAIMS:**

Claims 1 to 12. (Canceled).

13. (Currently Amended) A method for encrypting data according to an asymmetrical method using a processor, based on a factorization problem, comprising: ~~having~~

providing a public key to the processor; and

providing a private key to the processor; the public key being the iteration number $L$ as well as the composite number $n$~~, $n$ preferably being the product of a plurality of large prime numbers~~; the private key is made up of the factorization of $n$; the message $m = (m_1, m_2)$ to be encrypted is made up of at least the components $m_1$ *and* $m_2$; an encryption function $f(x)$ is iterated a total of $L$ times, with $c=(c_1,c_2)=f^L(m)$; $f(m)=(f_1(m),f_2(m))$ being applicable, and $f_1=(m_1 op_1 m_2)$mod $n$ as well as $f_2=(m_1, op_2 m_2)$mod $n$; ~~$op_1$ preferably being an addition and $op_2$ preferably being a multiplication;~~ the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the $L$-fold solution of a quadratic equation modulo $n$, it thereby being possible to retrieve the original message from the encrypted information $c = (c1, c2)$.

14. (Previously Presented) The method of claim 13, wherein a multivaluedness of the quadratic equation is eliminated by additional bits of $a_i$ und $b_i$.

15. (Previously Presented) The method of claim 14, wherein the multivaluedness of the quadratic equation is eliminated by calculating a parity and a Jacobi symbol which, particularly in the case of prime numbers of form 3 mod 4, can be communicated by 2 bits per iteration step.

16. (Currently Amended) The method of claim 13, wherein general iterations $f_1=(k_1 \cdot m_1+k_2 \cdot m_2)$mod $n$ as well as $f_2=k_3 \cdot m_1 \cdot m_2$ mod $n$ are used, ~~the~~ constants being part of the public key.

17. (Previously Presented) The method of claim 13, wherein the composite number $n$ as public key contains more than two factors.

18. (Previously Presented) The method of claim 13, wherein the message is now made up of an N-tuple $m=(m_1...m_N)$, the formula for the Lth iteration step using dependencies of $N$ values in each iteration step.

19. (Previously Presented) The method of claim 18, wherein the multivaluedness is resolved by additional bits that are derived from the values obtained in each iteration.

20. (Previously Presented) The method of claim 13, wherein the multivaluedness is resolved by redundancy in the transmitted data.

21. (Currently Amended) A method for generating a signature using a processor, comprising:

~~wherein~~ generating using the processor a signature ~~is generated~~ by interchanging the encryption and decryption steps, including functions for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; the public key being the iteration number $L$ as well as the composite number $n$~~, $n$ preferably being the product of a plurality of large prime numbers~~; the private key being made up of the factorization of $n$; the message $m = (m_1, m_2)$ to be encrypted being made up of at least the components $m_1$ *and* $m_2$; an encryption function $f(x)$ being iterated a total of $L$ times, with $c=(c_1,c_2)=f^L(m)$; $f(m)=(f_1(m),f_2(m))$ being applicable, and $f_1=(m_1op_1m_2)$mod $n$ as well as $f_2=(m_1,op_2m_2)$mod $n$; ~~$op_1$ preferably being an addition and $op_2$ preferably being a multiplication;~~ the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the $L$-fold solution of a quadratic equation modulo $n$, it thereby being possible to retrieve the original message from the encrypted information $c = (c1, c2)$.

22. (Currently Amended) A software for a computer, comprising:

functions for encrypting data according to an assymmetrical method being executed by a processor, based on a factorization problem, having a public key and a private key; the public key being the iteration number $L$ as well as the composite number $n$~~, $n$ preferably being the product of a plurality of large prime numbers~~; the private key being made up of the factorization of $n$; the message $m = (m_1, m_2)$ to be encrypted being made up of at least the components $m_1$ *and* $m_2$; an encryption function $f(x)$ being iterated a total of $L$ times, with $c=(c_1,c_2)=f^L(m)$; $f(m)=(f_1(m),f_2(m))$ being applicable, and $f_1=(m_1op_1m_2)$mod $n$ as well as $f_2=(m_1,op_2m_2)$mod $n$; ~~$op_1$ preferably being an addition and $op_2$ preferably being a multiplication;~~ the encryption function $f(x)$ being selected in such a way that the encryption

iteration can be reversed by the $L$-fold solution of a quadratic equation modulo $n$, it thereby being possible to retrieve the original message from the encrypted information $c = (c1, c2)$.

23. (Currently Amended) A data carrier for a computer, comprising:

~~the~~ storage of a software for ~~a~~ the computer, comprising functions for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; the public key being the iteration number $L$ as well as the composite number $n$~~, $n$ preferably being the product of a plurality of large prime numbers~~; the private key being made up of the factorization of $n$; the message $m = (m_1, m_2)$ to be encrypted being made up of at least the components $m_1$ and $m_2$; an encryption function $f(x)$ being iterated a total of $L$ times, with $c=(c_1,c_2)=f^L(m)$; $f(m)=(f_1(m),f_2(m))$ being applicable, and $f_1=(m_1 op_1 m_2) \bmod n$ as well as $f_2=(m_1, op_2 m_2) \bmod n$; ~~$op_1$ preferably being an addition and $op_2$ preferably being a multiplication;~~ the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the $L$-fold solution of a quadratic equation modulo $n$, it thereby being possible to retrieve the original message from the encrypted information $c = (c1, c2)$.

24. (Currently Amended) A computer system, comprising:

a device that allows the execution of a method, the method comprising: software for a computer, comprising functions for encrypting data according to an asymmetrical method, based on a factorization problem, having a public key and a private key; the public key being the iteration number $L$ as well as the composite number $n$~~, $n$ preferably being the product of a plurality of large prime numbers~~; the private key being made up of the factorization of $n$; the message $m = (m_1, m_2)$ to be encrypted being made up of at least the components $m_1$ and $m_2$; an encryption function $f(x)$ being iterated a total of $L$ times, with $c=(c_1,c_2)=f^L(m)$; $f(m)=(f_1(m),f_2(m))$ being applicable, and $f_1=(m_1 op_1 m_2) \bmod n$ as well as $f_2=(m_1, op_2 m_2) \bmod n$; ~~$op_1$ preferably being an addition and $op_2$ preferably being a multiplication;~~ the encryption function $f(x)$ being selected in such a way that the encryption iteration can be reversed by the $L$-fold solution of a quadratic equation modulo $n$, it thereby being possible to retrieve the original message from the encrypted information $c = (c1, c2)$.

25. (New) The method of claim 13, wherein $n$ is a product of a plurality of large prime numbers.

26. (New) The method of claim 25, wherein $op_1$ is an addition and $op_2$ is a multiplication.

27. (New) The method of claim 13, wherein $op_1$ is an addition and $op_2$ is a multiplication.

28. (New) The method of claim 21, wherein $n$ is a product of a plurality of large prime numbers, and $op_1$ is an addition and $op_2$ is a multiplication.

29. (New) The method of claim 22, wherein $n$ is a product of a plurality of large prime numbers, and $op_1$ is an addition and $op_2$ is a multiplication.

30. (New) The method of claim 23, wherein $n$ is a product of a plurality of large prime numbers, and $op_1$ is an addition and $op_2$ is a multiplication.

31. (New) The method of claim 24, wherein $n$ is a product of a plurality of large prime numbers, and $op_1$ is an addition and $op_2$ is a multiplication.